The University of Chicago

MAXIMAL ORDERS IN RATIONAL CYCLIC ALGEBRAS OF COMPOSITE DEGREE

A DISSERTATION SUBMITTED TO THE FACULTY
OF THE DIVISION OF THE PHYSICAL SCIENCES
IN CANDIDACY FOR THE DEGREE OF DOCTOR OF
PHILOSOPHY

DEPARTMENT OF MATHEMATICS

1938

By

SAM PERLIS

Private Edition, Distributed by
THE UNIVERSITY OF CHICAGO LIBRARIES
CHICAGO, ILLINOIS

Reprinted from
TRANSACTIONS OF THE AMERICAN MATHEMATICAL SOCIETY
Vol. 46, No. 1
July, 1939

The University of Chicago

MAXIMAL ORDERS IN RATIONAL CYCLIC ALGEBRAS OF COMPOSITE DEGREE

A DISSERTATION SUBMITTED TO THE FACULTY
OF THE DIVISION OF THE PHYSICAL SCIENCES
IN CANDIDACY FOR THE DEGREE OF DOCTOR OF
PHILOSOPHY

DEPARTMENT OF MATHEMATICS

1938

By

SAM PERLIS

Private Edition, Distributed by
THE UNIVERSITY OF CHICAGO LIBRARIES
CHICAGO, ILLINOIS

Reprinted from
TRANSACTIONS OF THE AMERICAN MATHEMATICAL SOCIETY
Vol. 46, No. 1
July, 1939

R. UNIV.
BIBLIOTHEEK
LEIDEN

MAXIMAL ORDERS IN RATIONAL CYCLIC ALGEBRAS OF COMPOSITE DEGREE*

BY
SAM PERLIS

Introduction. A maximal order M of a normal division algebra D over the rational number field may be imbedded† in a simple fashion in a maximal order of any normal simple algebra similar to D. When the normal simple algebra has degree greater than two, its class number is unity,‡ and it can then be shown that all maximal orders of the algebra are obtainable from any one by an inner automorphism of the algebra. Thus it is sufficient to determine a single M of each D in order to determine all maximal orders of all normal simple algebras of degree greater than two over the rational number field. This determination was made by Hull§ for the case in which the degree n of D is any odd prime, using methods similar to those of Albert|| for the case $n=2$. The methods and results of Hull are extended here to the case in which $n=\pi^e$ where π is any odd prime, and also to the case $n=2^e>2$ provided that D has odd discriminant and has the real number field as splitting field.

More specifically, it will be shown with the aid of the class field theory that each algebra D considered has a suitably normalized cyclic generation, and a maximal order of D will be expressed in terms of a finite number of quantities related to this generation. There are two chief points of difference between the present case and that of prime degree. The quantity σ in the normalized generation (Z, S, σ) is no longer the product of the primes ramified in D, but the product of certain powers of these primes. The exponents on these powers reduce to unity in the case of prime degree. The explicit basis given for the maximal order is similar to that for prime degree

* Presented to the Society, April 9, 1938; received by the editors October 13, 1938. While preparing this paper the author had the privilege of discussing some of its details with Professor A. A. Albert, and is grateful for this guidance and stimulus.

† For the concepts and results on the arithmetic of algebras see M. Deuring, *Algebren*, Ergebnisse der Mathematik und ihrer Grenzgebiete, vol. 4, no. 1.

‡ M. Eichler, *Bestimmung der Idealklassenzahl in gewissen normalen einfachen Algebren*, Journal für die reine und angewandte Mathematik, vol. 176 (1936), pp. 192–202.

§ Ralph Hull, *Maximal orders in rational cyclic algebras of odd prime degree*, these Transactions, vol. 38 (1935), pp. 514–530. For the case $n=2$ see Hull's paper in the same journal, vol. 40 (1936), pp. 1–11. Reference to the first of these papers will be made by the letter H.

|| A. A. Albert, *Integral domains of rational generalized quaternion algebras*, Bulletin of the American Mathematical Society, vol. 40 (1934), pp. 164–176.

except for the appearance of certain rational integral denominators which, again, reduce to unity in the case $n=\pi$.

For algebras of arbitrary degree, the determination may be reduced to the prime-power case if one can express maximal orders in a direct product of two normal division algebras of relatively prime degrees in terms of maximal orders in the two factors. A partial discussion of this direct product theory is given in the final section. The product of two orders, one in each factor, is an order in the direct product of the algebras, and it is shown that this order is maximal if and only if the discriminants of the two algebras are relatively prime. This result holds if any normal simple algebras are used instead of normal division algebras.

1. **Cyclic generations and related concepts.** A normal division algebra D of degree n over R is a cyclic algebra

$$D = (Z, S, \gamma) \tag{1}$$

and has a basis

$$u^{i-1}z_j, \qquad i, j = 1, \cdots, n, \tag{2}$$

where $(z_1, \cdots, z_n)$ is a basis of the cyclic field Z over R with generating automorphism S, and

$$u^n = \gamma, \qquad zu = uz^S \tag{3}$$

for every z of Z.

Since $(Z, S, \gamma) = (Z, S, \gamma\rho^n)$ for any rational number $\rho \neq 0$, it follows that the quantity γ of R may be assumed with no loss of generality to be a rational integer. If we choose for the basis $(z_1, \cdots, z_n)$ a minimal basis of Z, then the set of all linear combinations of the n^2 quantities (2) with coefficients rational integers is an order of D. This order is uniquely determined by the cyclic generation (1) of D and is called *the order I in D associated with this generation.* Every order of D, in particular an order I, is contained in a maximal order* of D. We shall obtain an infinite number of normalized cyclic generations of D and for each of the corresponding orders I we shall obtain n distinct maximal orders containing I.

A complete set of invariants of D under change of cyclic generation has been obtained by Hasse† in terms of the norm residue symbol

$$(\gamma, Z \mid q) = \left(\frac{\gamma, Z}{q}\right) = S^{\nu_q} \tag{4}$$

* Deuring, op. cit., p. 70.

† H. Hasse, *Theory of cyclic algebras over an algebraic number field*, these Transactions, vol. 34 (1932), pp. 171–214.

which is defined for every prime spot q of R. We shall adopt the convention that the integer ν_q is one of $0, 1, \cdots, n-1$. For any cyclic algebra $D_1=(Z_1, S_1, \gamma_1)$ of degree n over R, we have $(\gamma_1, Z_1|q)=S_1^{\nu_{1q}}$, and Hasse has shown that D_1 is equivalent to D if and only if $\nu_{1q}=\nu_q$ for every q. Hence the ν_q and the degree n form a complete set of invariants of D.

It is known that the norm residue symbol is the identity automorphism, that is, $\nu_q=0$, for all but a finite number of prime spots $q=q_1, \cdots, q_s$. These are precisely the prime spots for which the q-adic extension $D_q=D\times R_q$ is not total matric, and also are characterized as the prime factors of the discriminant of D. These prime spots $q_1, \cdots, q_s$ are called the *ramification spots* of D, and a cyclic algebra has at least two ramification spots unless it is total matric. The invariants ν_q satisfy the relations

$$\sum_q \nu_q \equiv 0 \pmod{n}, \qquad 2\nu_{q_\infty} \equiv 0 \pmod{n} \tag{5}$$

where q_∞ is the infinite prime spot of R, and these are the only relations between the invariants of an arbitrary cyclic algebra over R. However, a necessary and sufficient condition that a cyclic algebra D of prime-power degree $n=\pi^e$ over R be a division algebra is that at least one of its q-adic extensions be a division algebra, and this is equivalent to the condition that the corresponding invariant ν_q be prime to n. Both of these equivalent conditions follow readily from theorems* that (1) the q-index of $D=(Z, S, \gamma)$ over R is the order of the automorphism S^{ν_q} and thus is

$$n_q = n/(n, \nu_q); \tag{6}$$

and (2) the index of the cyclic algebra D is the least common multiple of all of its q-indices n_q.

Until §5 it will always be assumed that the normal division algebra D has prime-power degree $n=\pi^e>2$ over R so that there exists a ν_q which is prime to n. From (5) one obtains $\nu_{q_\infty}=0$ if n is odd (so that in this case q_∞ cannot be a ramification spot q_i), and $\nu_{q_\infty}\equiv 0 \pmod 2$ if $n=2^e>2$. In any case, ν_{q_∞} is not prime to n. Conditions (5) also imply that $s\geqq 2$ and that there must be at least two prime spots for which the corresponding invariants are prime to n. Hence we may hereafter let q_1 designate a ramification spot such that $(\nu_{q_1}, n)=1$ and $q_1\neq\pi$.

2. **Normalized cyclic generations.** Three lemmas will now be obtained for use in the proof of Theorem 1 which provides cyclic generations of an especially simple type for the algebra D. The first lemma defines a collection of fields from which the cyclic generation fields of D will be selected.

* Hasse, ibid., Theorem 5, p. 179, and (17.7), p. 203.

LEMMA 1. *For any prime $p \equiv 1 \pmod{2n}$ let H_p be the ideal group in R consisting of all principal ideals (r) where r is a rational number prime to p and is an n-ic residue modulo p. Then the class field Z_p corresponding to H_p is cyclic of degree n over R and has conductor p.*

If we let G_p be the group of all (r) with r prime to p and let g be a primitive root of p, we shall verify the decomposition

$$G_p = H_p + H_p g + \cdots + H_p g^{n-1}. \tag{7}$$

When $p \equiv 1 \pmod{2n}$, a quantity $\pm g^i$ is an n-ic residue modulo p if and only if i is a multiple of n, whence it follows that the cosets $H_p g^i$ are distinct. For any (r) in G_p we have $r = ab^{-1}$, a and b integers prime to p, $a = g^e + xp$, $b = g^f + yp$ with integers x and y. Then

$$r = \frac{g^f + x_1 p}{g^f + yp} g^{e-f} = r_1 g^{e-f} = \frac{g^e + xp}{g^e + y_1 p} g^{e-f}.$$

If $f \geqq e$, the number x_1 is an integer, and we have $r_1 \equiv 1 \pmod{p}$. Otherwise y_1 is integral and again we have the same congruence, so that (r_1) is in H_p and (r) is in $H_p g^{e-f}$, which is one of the cosets displayed. This verifies the decomposition above. The prime p is a generating modulus of the ideal group H_p so that the conductor of H_p, which is the g.c.d. of all the generating moduli, is either p or 1. Then clearly the conductor of H_p, and hence of Z_p, is p; and since G_p/H_p is cyclic of order n, the field Z_p is cyclic of degree n over R.

Since the next two lemmas depend on the notations of Theorem 1, the latter result will be stated now but not proved until the lemmas have been obtained.

THEOREM 1. *Let D be a normal division algebra of prime-power degree $n = \pi^e$ over the rational number field R, and let $q_1, \cdots, q_s$ be the finite ramification spots of D and n_i the q_i-index of D, $(i = 1, \cdots, s)$. Then, if π is odd, there are infinitely many cyclic fields Z of degree n over R such that*

(a) $D = (Z, S, \sigma)$, $\sigma = \prod_{i=1}^{s} q_i^{n/n_i}$;

(b) *Z has conductor a prime p such that $p \equiv 1 \pmod{n}$, $(p, \sigma) = 1$;*

(c) *$q_1, \cdots, q_s$ generate prime ideals (q_i) in Z;*

(d) *σ is an n-ic residue modulo p.*

If $n = 2^e > 2$ the same results hold provided that D is unramified at the prime spot 2 and at the infinite prime spot q_∞.

Let ν_∞ and $\nu_1, \cdots, \nu_s$ be the invariants corresponding to q_∞ and the q_i. As we have already seen, our hypotheses imply that $\nu_\infty = 0$. By (6) we have $n_i = n/(n, \nu_i)$, and the congruences

$$-\nu_1 n n_i^{-1} x_i \equiv \nu_i \pmod{n}, \qquad i = 2, \cdots, s, \tag{8}$$

have solutions x_i since $(n, \nu_1) = 1$ and $(n, \nu_1 n n_i^{-1}) = (n, n n_i^{-1}) = n n_i^{-1} = (n, \nu_i)$. Note that the x_i are prime to n. Let ζ be a primitive nth root of unity; let

$$\alpha_i = (q_1^{x_i} q_i)^{n/n_i}, \qquad i = 2, \cdots, s, \tag{9}$$

$$F = R(\zeta), \qquad K = F(\alpha_2^{1/n}, \cdots, \alpha_s^{1/n}). \tag{10}$$

LEMMA 2. *The field $K_1 = K(q_1^{1/\pi})$ has degree π over K.*

Consider an equation

$$q_1^{c_1}(q_1^{x_2} q_2)^{c_2} \cdots (q_1^{x_s} q_s)^{c_s} = a^n, \qquad a \text{ in } F, \tag{11}$$

where the c_i are integers to be determined, and suppose that π is not one of the q_i. Then all the q_i are unramified in F since the discriminant of F is a power* of π. Hence the prime ideal factorization of the quantities in (11) shows that $c_1 + c_2 x_2 + \cdots + c_s x_s$ and $c_2, \cdots, c_s$ are all divisible by n, and therefore c_1 is divisible by n. Thus (11) holds only when the exponents c_i are all multiples of n, a property which implies† that the composite of the fields $F(q_1^{1/n})$ and $F([q_1^{x_i} q_i]^{1/n})$ for $i = 2, \cdots, s$ is their direct product. These s fields have subfields $F(q_1^{1/\pi})$ and $F(\alpha_i^{1/n})$ for $i = 2, \cdots, s$, respectively, and the composite of these subfields must be their direct product. Then the degree of K_1 over K is the degree of $F(q_1^{1/\pi})$ over F, and this is either‡ π or 1. If the degree were 1, then F would contain $q_1^{1/\pi}$, q_1 would be the πth power of an ideal in F, whereas q_1 is prime to π and hence unramified in F. We have proved the lemma for the case in which π is not one of the q_i.

In case π is one of the q_i, we have assumed $\pi > 2$ and may take $\pi = q_2$. Consider an equation of the form (11) with the factor $q_1^{c_1}$ deleted, and obtain $c_2 x_2 + \cdots + c_s x_s \equiv c_3 \equiv \cdots \equiv c_s \equiv 0 \pmod{n}$ since q_1 and $q_3, \cdots, q_s$ are unramified in F. Thus $c_2 x_2$ is divisible by n, x_2 is prime to n, and $c_2 \equiv 0 \pmod{n}$. As in the previous paragraph, the composite K_0 of the fields $F([q_1^{x_i} q_i]^{1/n})$ for $i = 2, \cdots, s$ is then their direct product and (by Bericht II, p. 43) any cyclic subfield of K_0 has the form

$$F([(q_1^{x_2} q_2)^{d_2} \cdots (q_1^{x_s} q_s)^{d_s}]^{1/n}), \qquad d_i \text{ integers}. \tag{12}$$

If $F(q_1^{1/\pi})$ is contained in K_0, it must have the form (12) so that§

* R. Fricke, *Lehrbuch der Algebra*, 1928, vol. 3, p. 195.

† H. Hasse, *Bericht über neuere Untersuchungen und Probleme aus der Theorie der algebraischen Zahlkörper, Teil* II, Jahresbericht der deutschen Mathematiker-Vereinigung, supplementary vol. 6 (1930), p. 43. Parts I and Ia of this article appeared in the Jahresbericht, vols. 35 and 36. These papers will be designated here as Bericht I, Ia, and II.

‡ Bericht II, p. 42, Theorem I.

§ Bericht II, p. 42, Theorem II.

$$q_1^{n/\pi} = c^n q_1^{(x_2d_2+\cdots+x_sd_s)x}\pi^{d_2x}\cdot q_3^{d_3x}\cdots q_s^{d_sx}$$

with c in F. By considering prime ideal factorizations of the quantities in this equation, we find that $d_3x, \cdots, d_sx$ are divisible by n, $x_2d_2x+\cdots+x_sd_sx \equiv x_2d_2x \equiv n/\pi \pmod{n}$, x_2 is prime to n, $d_2x \equiv x_0n/\pi \pmod{n}$. The equation above then takes the form

$$q_1^{n/\pi} = c_0^n q_1^{n/\pi}\pi^{x_0n/\pi}, \qquad c_0^{-n} = \pi^{x_0n/\pi}.$$

Since x_0 is prime to n we easily obtain $\pi^{n/\pi} = c_{01}^n$ with c_{01} in F and thus have $\pi^{1/\pi}$ in F. Then F must contain the non-normal subfield $R(\pi^{1/\pi})$ whereas F is cyclic and all of its subfields are normal over R. We have shown that $F(q_1^{1/\pi})$ is not contained in K_0. Then it is not contained in the subfield K of K_0 and the lemma is proved.†

LEMMA 3. *There are infinitely many rational primes p such that $p \equiv 1 \pmod{2n}$, $(p, \sigma) = 1$, and*

(e) *$\alpha_2, \cdots, \alpha_s$ are n-ic residues modulo p;*

(f) *q_1^t is an n-ic non-residue modulo p for $t = 1, \cdots, n-1$.*

The field K_1 of Lemma 2 is cyclic of degree greater than 1 over K and is class field to an ideal group H_1 in K. In any ideal class different from the identity class H_1, we may select an infinite number of prime ideals P which are of degree one, prime to σ, and prime to the different of K over R. An infinite number of rational primes $p = N_{K|R}(P)$ is thus defined. Every such p is prime to σ; and since the prime ideal factors of p in F must have degree one, it follows that $p \equiv 1 \pmod{n}$. Then $p \equiv 1 \pmod{2n}$ if n is odd.

When $n = 2^e$ we shall make the following additional restrictions in the choice of the ideals P. Let F_2 be the root field over R of the equation $x^{2n} = 1$ so that F_2 has degree two over F. The field K cannot contain F_2 since then F_2 would have the form (12) which leads to a contradiction. Hence the composite (K, F_2) has degree two over K and is the class field corresponding to an ideal group H_2 in K. We wish to choose ideals P lying outside of H_1 as before but also lying in H_2. Let these ideal groups have a common generating modulus. Then H_1 and H_2 are collections of ray classes, and we must verify that the ray classes comprising H_2 do not all lie among those comprising H_1. This fact is clearly true since otherwise $(K, F_2) = K_1$, $K(\zeta^{1/2}) = K(q_1^{1/2})$, which is impossible. Thus there is a ray class C in H_2 but not in H_1, and C contains infinitely many prime ideals with the properties of the previous paragraph.

† Since $(q_1^{x_2}\pi)^{1/n_2}$ is in K, this field contains $q_1^{1/\pi}$ if and only if it contains $\pi^{1/\pi}$. Then we see that Lemma 2 is false without the hypothesis that $\pi \neq 2$ when π is one of the q_i. For, if $\pi = 2$, take $n \geqq 8$ and see that F, and hence K, contains a primitive eighth root ζ_0 of unity and thus contains $\zeta_0 - \zeta_0^3 = 2^{1/2}$, so that $q_1^{1/2}$ is in K and the lemma fails.

The norms of these ideals are rational primes p such that $p \equiv 1 \pmod{2n}$ since they are unramified in F_2 and their prime ideal factors in F_2 have degree one.

The proofs of properties (e) and (f) are similar to corresponding proofs in H and will be omitted here.* To prove Theorem 1, let p be any prime of Lemma 3 and let Z be the corresponding field Z_p of Lemma 1. Then property (b) of the theorem holds. Property (f) of the last lemma is equivalent to the statement that q_1 is a prime ideal in Z, and property (e) implies that the α_i are in the ideal group H_p corresponding to Z. Expressed in terms of Artin symbols these facts yield

$$(13) \qquad (Z/\alpha_i) = I, \qquad (Z/q_1)^{x_i n/n_i} = (Z/q_i)^{-n/n_i}.$$

Since x_i is prime to n and the automorphism (Z/q_1) has order n, it follows that $(Z/q_1)^{x_i n/n_i}$ has order n_i. A simple computation shows that (Z/q_i) has order n, which is equivalent to (c). Applying (e) together with (8) and (5), we are led to (d).

The Artin symbol $A = (Z/q_1)$ is a generating automorphism of Z over R, and the equation $S^{\nu_1} = A^{-1}$ defines another generating automorphism S. Then (Z, S, σ) is a cyclic algebra of degree n. A computation following the pattern in H shows that D and (Z, S, σ) have the same invariants, yielding (a) and completing the proof of the theorem.

3. **Some properties of Z.** Since Z is cyclic over R with conductor p, it is a subfield† of the cyclotomic field $R(\xi)$, where ξ is a primitive pth root of unity. The field $R(\xi)$ is cyclic over R so that Z is its unique subfield of degree n, and Z is thus uniquely determined by its degree n, its prime conductor p, and the property of being an abelian field over R. Write $p = 1 + hn$, and let g be a primitive root of p. Then a normal basis of Z is given by‡

$$\eta_0, \eta_1, \cdots, \eta_{n-1}$$

with

$$(14) \qquad \eta_i = \xi_i + \xi_{i+n} + \cdots + \xi_{i+(h-1)}, \quad \xi_k = \xi^{g^k},$$

* We may observe that Lemma 3 is actually false without the assumption $\pi \neq 2$ when π is one of the q_i. For, without this assumption we may have $n = 2^e$, $K \geqq F(q_1^{1/2}) = K_0$, and $H \leqq H_0$, where H and H_0, respectively, are the ideal groups in F corresponding to the class fields K and K_0 over F. The condition $p \equiv 1 \pmod{n}$ implies that any prime factor P of p in F has degree 1, and condition (e) implies that P is in H and hence in H_0. Then any prime factor P_0 of P in K_0 has degree 1; hence the quantity $q_1^{1/2}$ of K_0 satisfies $q_1^{1/2} \equiv y \pmod{P_0}$ with y in R. Then $q_1^{n/2} \equiv y^n \pmod{P_0}$ so that we have $q_1^{n/2} \equiv y^n \pmod{p}$, a contradiction with (f).

The falsity of Lemma 3 can be seen to imply the falsity of the conclusions in Theorem 1. Thus the restrictive assumption in Theorem 1 is necessary.

† Bericht I, p. 39.

‡ B. L. van der Waerden, *Moderne Algebra*, 1930, vol. 1, pp. 160 ff.

for $i=0, \cdots, n-1$ and $k=0, 1, \cdots, p-2$. Hence $Z=R(\eta_i)$ for any i, and a generating automorphism of Z over R is induced by

$$U: \qquad \xi \longleftrightarrow \xi^g.$$

Clearly, U is a generating automorphism of the cyclic group $[U]$ of $R(\xi)$ over R, and $[U^n]$ is the group of $R(\xi)$ over Z.

The factorization of p in Z may now be obtained. Define

$$\beta = \prod_{t=0}^{h-1} (1 - \xi^{g^{nt}}). \tag{15}$$

Then β is unaltered by U^n and hence is in Z, and a direct computation shows that $N_{Z|R}(\beta)=p$. The principal ideal $P=(\beta)$ is thus a prime ideal of Z and is a factor of p. But p is completely ramified in the cyclotomic field $R(\xi)$ and hence in the subfield Z, so that $p=P^n$. This fact and Theorem (14) of §8, Bericht Ia, may be used to show that the discriminant of Z over R is p^{n-1}. We thus have

THEOREM 2. *Each field Z of Theorem* 1 *(and Z_p of Lemma* 1*) has discriminant p^{n-1}. The factorization of p in Z is*

$$p = P^n, \qquad P = (\beta), \qquad N_{Z|R}(\beta) = p,$$

where β is given by (15).

The quantity β will be used in the next section when basal elements of maximal orders are defined.

4. **Maximal orders in D.** The algebra D has the form

$$D = Z + uZ + \cdots + u^{n-1}Z, \qquad u^n = \sigma,$$

and this generation of D is associated with an order

$$I = Z_0 + uZ_0 + \cdots + u^{n-1}Z_0 \tag{16}$$

where Z_0 is the maximal order of Z. We shall display n distinct maximal orders in D which contain I. These n orders are defined in terms of n rational integers λ given in

LEMMA 4. *The simultaneous congruences*

$$\lambda^n \equiv \sigma \pmod{p}, \qquad \lambda \equiv 0 \pmod{\sigma} \tag{17}$$

have exactly n solutions λ which are incongruent modulo p.

Any solution of the second congruence has the form $\lambda_0\sigma$. If this is substituted in the first congruence, there results

$$\lambda_0^n \equiv \sigma\sigma_1^n \pmod{p} \tag{18}$$

with $\sigma\sigma_1 \equiv 1 \pmod{p}$. There exists a solution of (18) if and only if* we have $(\sigma\sigma_1{}^n)^{(p-1)/g} \equiv 1 \pmod{p}$ where $g=(p-1, n)$; then the exact number of incongruent solutions is g. In the present case $g=n$, and the first congruence in (17) has a solution, by Theorem 1, so that $\sigma^{(p-1)/n} \equiv 1 \pmod{p}$. Also, $\sigma_1{}^{p-1} \equiv 1 \pmod{p}$ so that

$$\sigma^{(p-1)/n}\sigma_1{}^{p-1} = (\sigma\sigma_1^n)^{(p-1)/n} \equiv 1 \pmod{p},$$

and the lemma is proved.

We shall consider modules of the form

$$M = Z_0 + y\tau_1^{-1}Z_0 + \cdots + y^{n-1}{}^{-1}\tau_{n-1}Z_0 \tag{19}$$

where

$$y = (\lambda - u)\beta^{-1} \tag{20}$$

with λ satisfying (17), β given by (15), and where the τ_j are rational integers such that

$$\tau_{n-1} \text{ divides } \sigma, \qquad \tau_i \text{ divides } \tau_{i+1} \tag{21}$$

for $i=1, \cdots, n-2$. The τ_j will be chosen so that M is a ring. First, for any a_0 in Z_0 we find by a simple computation that $a_0y=(a_0-a_0{}^S)\lambda\beta^{-1}+ya_0{}^S$. The ramification order of p in Z over R is n so that the inertial group of p in Z over R is the complete galois group of Z over R. Hence $a_0 \equiv a_0{}^S \pmod{\beta}$ and we have $a_0y=ya_0{}^S+a_1\lambda$, (a_1 in Z_0). A simple induction then yields

Lemma 5. *For every a_0 in Z_0 and every integer $i>0$ we have*

$$a_0y^i = y^ia_0{}^{S^i} + y^{i-1}a_1\lambda + \cdots + a_i\lambda^i, \qquad a_j \text{ in } Z_0.$$

By means of an n-rowed matrix representation of D it may be verified† that the characteristic function of y is

$$t^n - \lambda\delta_1t^{n-1} + \lambda^2\delta_2t^{n-2} - \cdots + (-\lambda)^{n-1}\delta_{n-1}t + (-1)^n\delta_n \tag{22}$$

where δ_n is the rational integer $\delta_n=(\lambda^n-\sigma)p^{-1}$ and, for $i<n$, δ_i is the ith elementary symmetric function of β^{-1} and its conjugates. The ith elementary symmetric function of the algebraic integer $p\beta^{-1}$ and its conjugates in Z is $p^i\delta_i$ which must then be a rational integer. Since $p^i\delta_i$ is divisible by

$$P^{i(n-1)} = P^{(i-1)n+n-i} = (p^{i-1})P^{n-i},$$

it follows that $p\delta_i$ is a rational integer divisible by P^{n-i} and hence by p when $i<n$. This proves that all of the coefficients of (22) are rational integers.

* L. E. Dickson, *Introduction to the Theory of Numbers*, 1931, p. 31, exercise 5.

† See H, p. 525.

Observe that the coefficient δ_n in (22) has the property that $\delta_n\sigma^{-1}$ is an integer prime to σ. An induction based on (22) yields

LEMMA 6. *For* $k=0, 1, \cdots, n-2$ *we have*

$$y^{n+k} = y^{n-1}a_1 + y^{n-2}a_2 + \cdots + a_n$$

with rational integral coefficients a_j *such that*

$$a_j \equiv 0 \pmod{\lambda^{k+j}}, \qquad j = 1, \cdots, n-k-1,$$

$$a_{n-k} \equiv 0 \pmod{\sigma}, \qquad (a_{n-k}\sigma^{-1}, \sigma) = 1,$$

and, if $k>0$,

$$a_j \equiv 0 \pmod{\lambda^{k+j+1-n}}, \qquad j = n-k+1, \cdots, n.$$

Thus every a_j *is divisible by* σ.

The module $M=Z_0+\sum_{i=1}^{n-1}y^i\tau_i^{-1}Z_0$ of (19) contains the set MZ_0, that is, all sums of products aa_0 with a in M and a_0 in Z_0. By Lemma 5, (21), and the fact that λ is divisible by σ, we see also that the sets $Z_0y^i\tau_i^{-1}$ are all contained in M so that $Z_0y^i\tau_i^{-1}Z_0 \leqq M, Z_0M \leqq M$. Thus M is a ring if and only if we have

$$y^i\tau_i^{-1}M \leqq M, \qquad i = 1, \cdots, n-1. \tag{23}$$

This is equivalent to the condition

$$y^i\tau_i^{-1}y^j\tau_j^{-1} = y^{i+j}(\tau_i\tau_j)^{-1} \text{ in } M, \qquad i, j = 1, \cdots, n-1. \tag{24}$$

When $i+j<n$, the condition (24) holds if and only if $\tau_i\tau_j$ divides τ_{i+j}. Otherwise $i+j=n+k$, $(k=0, 1, \cdots, n-2)$, and, by Lemma 6, (24) holds if and only if $\tau_i\tau_j$ divides each quantity $a_r\tau_{n-r}$, $(r=1, \cdots, n)$, where we define $\tau_0=1$. In particular, it is sufficient to have

$$\sigma^{k+r}\tau_{n-r} \equiv 0 \pmod{\tau_i\tau_j}, \qquad r = 1, \cdots, n-k-1, \tag{25}$$

$$\sigma^{k+r+1-n}\tau_{n-r} \equiv 0 \pmod{\tau_i\tau_j}, \qquad r = n-k, \cdots, n. \tag{26}$$

Since $\tau_i\tau_j$ divides σ^2, (25) holds when $k+r\geqq 2$. Otherwise $r=1$, $k=0$, and (25) becomes $\sigma\tau_{n-1}\equiv 0 \pmod{\tau_i\tau_j}$ which by (21) is satisfied. In (26) we have $k+r\geqq n$, and see that the condition is not restrictive when $k+r>n$, $k+r+1-n\geqq 2$. We have proved

LEMMA 7. *Sufficient conditions that the module* M *of* (19) *be a ring are given by the following congruences*:

$$\tau_{i+j} \equiv 0 \pmod{\tau_i\tau_j}, \qquad i+j<n, \tag{27}$$

$$\sigma\tau_{i+j-n} \equiv 0 \pmod{\tau_i\tau_j}, \qquad i+j\geqq n. \tag{28}$$

Let us now make the definition $\tau_0=1$,

$$\tau_j = \prod_{i=1}^{s} q_i^{e_i}, \qquad e_i = \left[\frac{j}{n_i}\right] \tag{29}$$

for $j=1, \cdots, n-1$, and verify that this choice of the τ_j satisfies the conditions* of Lemma 7. The quantity $\tau_a\tau_b$ is exactly divisible by $q_{i0}=q_i^{e+f}$, $e=[a/n_i]$, $f=[b/n_i]$. If $a+b<n$, the quantity τ_{a+b} is exactly divisible by q_i^g, $g=[(a+b)/n_i]\geqq e+f$, so that (27) holds. If $a+b\geqq n$, then τ_{a+b-n} has the exact factor q_i^g,

$$g = \left[\frac{a+b-n}{n_i}\right] = \left[\frac{a+b}{n_i}\right] - \frac{n}{n_i} \geqq e+f-\frac{n}{n_i}.$$

But σ has the factor q_i^{n/n_i}, $\sigma\tau_{a+b-n}$ has $q_i^{g+n/n_i}\geqq q_i^{e+f}$ as factor, so that (28) holds. We have proved that M is a ring.

The ring M is a linear set of finite order over the domain of all rational integers; it contains Z_0 and hence all rational integers; and it contains $u=\lambda-y\beta$ and hence a basis $u^{i-1}z_j$, $(i, j=1, \cdots, n)$, of D where the z_j form any integral basis of Z. These properties imply† that the quantities of M are all integral and that M is an order of D. This order is maximal in D if and only if‡ its discriminant is the discriminant§

$$\prod_{i=1}^{s} q_i^{n^2(n_i-1)/n_i} \tag{30}$$

of the algebra D.

The sets M and I have respective bases w and v given by the vectors

$$w = (z_1, \cdots, z_n, \tau_1^{-1}yz_1, \cdots, \tau_1^{-1}yz_n, \cdots, \tau_{n-1}^{-1}y^{n-1}z_n) = (w_1, \cdots, w_{n^2}),$$
$$v = (z_1, \cdots, z_n, uz_1, \cdots, uz_n, \cdots, u^{n-1}z_n) = (v_1, \cdots, v_{n^2}),$$

where the z_j form an integral basis of Z. There is a nonsingular matrix B with rational elements such that $w=vB$, and the discriminant of M is then

$$\Delta(w) = |T(w_iw_j)| = \Delta(v)\cdot|B|^2.$$

Here $\Delta(v)$ is the discriminant $|T(v_iv_j)|$ of the basis v, and|| $\Delta(v)=(\sigma p)^{n(n-1)}$. To compute $|B|^2$ we observe¶ that when the matrix B is expressed as an

* Note that this choice of the τ_j makes $\tau_1, \cdots, \tau_{n_i-1}$ prime to q_i. Hence $\tau_1=\cdots=\tau_{n-1}=1$.

† Deuring, op. cit., p. 71, Theorem 9.

‡ E. Artin, *Zur Arithmetik hyperkomplexer Zahlen*, Abhandlungen aus dem mathematischen Seminar der Hamburgischen Universität, vol. 5 (1928), p. 265.

§ Reichhardt, *Die Diskriminante einer normalen einfachen Algebra*, Journal für die reine und angewandte Mathematik, vol. 173 (1935), pp. 31–34.

|| See H, p. 523.

¶ Ibid., p. 526.

n-rowed matrix whose elements are $n\times n$ matrices B_{ij}, then every B_{ij} below the main diagonal is a zero matrix, B_{11} is an identity matrix, and every matrix B_{jj}, $(j>1)$, has determinant equal, except possibly for sign, to the norm

$$[N(\tau_{j-1}\beta\beta^S\cdots\beta^{S^{j-2}})]^{-1}=(\tau_{j-1}^n p^{j-1})^{-1}.$$

Then $|B|^2=|B_{11}B_{22}\cdots B_{nn}|^2$ has the value

$$|B|^2=(\tau_1\cdots\tau_{n-1})^{-2n}p^{-n(n-1)}$$

so that $\Delta(w)=\sigma^{n(n-1)}(\tau_1\cdots\tau_{n-1})^{-2n}$. But

$$\tau_1\cdots\tau_{n-1}=\prod_{i=1}^{s}q_i^{[(n/n_i-1)+(n/n_i-2)+\cdots+1]n_i}=\prod q_i^{(n/n_i-1)n/2}$$

and $\Delta(w)=\prod q_i^{n^2(n_i-1)/n_i}$ which is the formula (30) for the discriminant of D. Thus M is a maximal order of D.

THEOREM 3. *Let D be an algebra of Theorem* 1 *with normalized cyclic generation (Z, S, σ) as described in that theorem, $D=Z+uZ+\cdots+u^{n-1}Z$, $u^n=\sigma$. Then n distinct maximal orders in D are given by the modules*

$$M(\lambda)=Z_0+y\tau_1^{-1}Z_0+\cdots+y^{n-1}\tau_{n-1}^{-1}Z_0,$$

where Z_0 is the maximal order of Z, the τ_i are rational integers defined by (29), *and $y=(\lambda-u)\beta^{-1}$, with β defined by* (15) *and λ varying over the n rational integers defined by* (17). *Each $M(\lambda)$ contains the order*

$$I=Z_0+uZ_0+\cdots+u^{n-1}Z_0$$

associated with the cyclic generation (Z, S, σ) of D.

That $M(\lambda_1)$ is distinct from $M(\lambda_2)$ was proved in H, p. 527, by showing that the corresponding quantities $y=y_1$, $y=y_2$ are such that y_1-y_2 is not integral.

5. **Maximal orders in direct products.** In view of the factorization of any normal division algebra D into a direct product of normal division algebras D_i whose degrees are powers of distinct primes, we may inquire whether maximal orders of D can be obtained simply in terms of those of the D_i. We shall solve this problem under certain hypotheses on the D_i and shall obtain some further results on the general problem.

Let A_1 and A_2 be cyclic algebras of relatively prime degrees over R and $A=A_1\times A_2$. A ramification spot of A must be a ramification spot for one of the A_i. Conversely, suppose that one of the A_i does not split at q. Then A_{1q} and A_{2q} have indices d_1 and d_2 which are relatively prime and one of which

is greater than unity. Hence A_q has index $d_1d_2>1$. Thus the ramification spots of A are those of A_1 together with those of A_2.

If A_1 and A_2 have cyclic generation fields Z_1 and Z_2, respectively, then A has the cyclic generation field $Z_1\times Z_2$. This fact will be used several times in this section and may be verified by a direct computation and also, for algebras over R, in the following way.

LEMMA 8. *Let* $A_i=(Z_i, S_i, \sigma_i)$ *be a cyclic algebra of degree* m_i *over* R, $(i=1, 2)$, *where* $(m_1, m_2)=1$. *Then* $A=A_1\times A_2$ *has a cyclic generation* $A=(Z, S, \sigma)$ *where* $Z=Z_1\times Z_2$, $S=S_1S_2$, $\sigma=\sigma_1^{m_2}\sigma_2^{m_1}$.

The composite of the Z_i is their direct product, so that (Z, S, σ) has degree m_1m_2 over R. If the invariants of A_i are denoted by ν_{iq} for every prime spot q and those of A by ν_q, then*

$$\nu_q \equiv m_2\nu_{1q} + m_1\nu_{2q} \pmod{m_1m_2}.$$

We have

$$(\sigma, Z \mid q) = \prod_{i,j} (\sigma_i, Z_j \mid q)^{m_1m_2/m_i} = \prod_i (\sigma_i, Z_i \mid q)^{m_1m_2/m_i}$$
$$= S_1^{m_2\nu_{1q}}S_2^{m_1\nu_{2q}} = (S_1S_2)^{m_2\nu_{1q}+m_1\nu_{2q}} = S^{\nu_q}.$$

Hence (Z, S, σ) has the same invariants ν_q and degree m_1m_2 as A. Thus the lemma is proved.

Let J_1 and J_2 be any orders in A_1 and A_2, respectively, and consider the product J_1J_2 in $A_1\times A_2$, consisting of all sums of products a_1a_2 with a_i in J_i. The set $J=J_1J_2$ is an order in A as one can easily verify. If bases of J_1 and J_2 over the rational integers are given by $(u_1, \cdots, u_{m_1^2})$ and $(v_1, \cdots, v_{m_2^2})$, respectively, J_1J_2 has a basis $(u_1v_1, \cdots, u_iv_j, \cdots, u_{m_1^2}v_{m_2^2})$.

LEMMA 9. *If* J_i *has discriminant* Δ_i, $(i=1, 2)$, *then* $J=J_1J_2$ *has discriminant* $\Delta_0=\Delta_1^{m_2^2}\Delta_2^{m_1^2}$.

The basis given above for J may be designated by $(w_1, \cdots, w_{m_1^2m_2^2})$, and then $\Delta_0=|T(w_xw_y)|$ where T is the trace function in A. Let T_i be the trace in A_i, and let a_i be any element of A_i. We shall show that $T(a_1a_2)=T_1(a_1)T_2(a_2)$.

Let W_i be a basis of A_i relative to a cyclic generation field Z_i of A_i for $i=1, 2$. Then the equation of $a_iW_i=W_iB_i$ defines a set of matrices B_i, with elements in Z_i, forming an algebra equivalent to A_i under the correspondence $a_i\longleftrightarrow B_i$ for every a_i of A_i, and $T_i(a_i)$ is defined to be the trace of the matrix B_i. Since m_1 and m_2 are relatively prime, the composite $Z=Z_1\times Z_2$ is a cyclic generation field of A, and a basis of A relative to Z is given by the vector W

* Hasse, *Theory of cyclic algebras over an algebraic number field*, loc. cit., p. 179, Theorem 4.

consisting of the products of each of the elements of W_1 by each of W_2. Then $aW = WB$ defines a representation $a \longleftrightarrow B$ of A, and $T(a)$ is the trace of the matrix B. We write $W_i = (w_{i1}, \cdots, w_{im_i})$ and have

$$a_1 w_{1r} = \sum_f w_{1f} b_{1fr}, \qquad a_2 w_{2t} = \sum_g w_{2g} b_{2gt},$$

$$a_1 w_{1r} a_2 w_{2t} = a_1 a_2 w_{1r} w_{2t} = \sum_{f,g} w_{1f} w_{2g} b_{1fr} b_{2gt}.$$

Hence the matrix B corresponding to $a = a_1 a_2$ has elements $b_{1fr} b_{2gt}$ and has, as desired, the trace

$$T(a_1 a_2) = \sum_{r,t} b_{1rr} b_{2tt} = \left(\sum_r b_{1rr} \right) \left(\sum_t b_{2tt} \right) = T_1(a_1) T_2(a_2).$$

Since $w_x w_y = u_i v_h u_j v_k$, we may write $T(w_x w_y) = T(u_i u_j v_h v_k) = T_1(u_i u_j) T_2(v_h v_k)$. Consider the matrices $C_1 = (T_1(u_i u_j))$ and $C_2 = (T_2(v_h v_k)) = (c_{hk})$. The discriminant $|T(w_x w_y)|$ of J is the determinant $\Delta_0 = |C_1 c_{hk}|$ of a matrix which we have written as a square matrix of $m_2^2 = k_2$ rows whose elements are square matrices of $m_1^2 = k_1$ rows. When C_2 is one-rowed, we have $|C_1 c_{hk}| = |C_1|^{k_2} |C_2|^{k_1}$ since then $k_2 = 1$, and we now assume that this formula holds for all matrices C_2 of $k_2 - 1$ rows. We may assume $c_{11} \neq 0$ and then may replace the blocks $C_1 c_{h1}$ by zero matrices under elementary transformations which replace the blocks $C_1 c_{hk}$ by $C_1 d_{hk}$, $d_{hk} = c_{hk} - c_{h1} c_{1k} c_{11}^{-1}$. In the remainder of this paragraph the subscripts h and k on c_{hk} will vary over $1, \cdots, k_2$ and those on d_{hk} will vary over $2, \cdots, k_2$. We have

$$\Delta_0 = |C_1 c_{hk}| = |C_1 c_{11}| \cdot |C_1 d_{hk}| = |C_1| \cdot c_{11}^{k_1} \cdot |C_1|^{k_2 - 1} \cdot |d_{hk}|^{k_1}$$

by our induction. But $|c_{hk}| = c_{11} |d_{hk}|$ so that $\Delta_0 = |C_1|^{k_2} \cdot |C_2|^{k_1}$, and the lemma is proved.

The discriminant of A is the product*

$$\Delta = \prod_q q^{e_q}, \qquad e_q = (n_q - 1) n^2 / n_q,$$

where q varies over all ramification spots of A, n is the degree $m_1 m_2$ of A, and n_q is the q-index of A. Then $n_q = m_{1q} m_{2q}$ where m_{iq} is the q-index of A_i. Let Δ_i be the discriminant of A_i. Then a direct computation shows that if A_1 and A_2 have no ramification spots in common, the discriminant of A is $\Delta_1^{m_2^2} \Delta_2^{m_1^2}$. Otherwise the Δ_i have common factors q, and in fact we find that in general A has discriminant

$$\Delta = \Delta_1^{m_1^2} \Delta_2^{m_2^2} \prod_q q^{-(m_{1q}-1)(m_{2q}-1) n^2 / n_q}$$

* Reichhardt, op. cit.

where the product is taken over all common ramification spots q of A_1 and A_2. An immediate consequence of this formula and Lemma 9 is stated now.

THEOREM 4. *Let A_1 and A_2 be normal simple algebras of relatively prime degrees m_1 and m_2 over R, and let M_1 and M_2 be any maximal orders in A_1 and A_2, respectively. Then M_1M_2 is a maximal order in $A=A_1\times A_2$ if and only if the discriminants Δ_1 and Δ_2 of A_1 and A_2 are relatively prime. In this case the discriminant of A is $\Delta_1^{m_2^2}\Delta_2^{m_1^2}$.*

This is an analogue of a known theorem* on algebraic fields over R with relatively prime discriminants. That $M=M_1M_2$ is maximal may also be proved by using Hasse's determination† of all maximal orders in the q-adic algebra A_q. We show by this means that for every prime spot q the q-component M_q is a maximal order of A_q. But this is a necessary and sufficient condition that M be maximal in A.

An application of Lemma 8 and Theorem 1 yields the following result which may be useful in the determination of maximal orders in a direct product.

THEOREM 5. *Let D be a direct product $D_1\times\cdots\times D_t$ of normal division algebras D_i of Theorem* 1 *such that the degrees m_i of the D_i are relatively prime in pairs, and let $n=m_1\cdots m_t$. Then each D_i has a cyclic generation (Z_i, S_i, σ_i) as described in Theorem* 1, *and D has a cyclic generation*

$$D=(Z,S,\sigma),\quad Z=Z_1\times\cdots\times Z_t,\quad S=S_1\cdots S_t,\quad \sigma=\prod_i \sigma_i^{n/m_i}.$$

The generations of the D_i may be chosen so that the conductors $p_1,\cdots,p_t$ of $Z_1,\cdots,Z_t$ are distinct primes, and are not ramification spots of D. The former property implies that the maximal order Z_0 of Z is the product of the maximal orders Z_{0i} of the fields Z_i.

* D. Hilbert, *Gesammelte Abhandlungen*, vol. 1, 1932, p. 146. The result of Theorem 4 was also obtained in a different way by K. Shoda and T. Nakamura in the paper *Über das Produkt zweier Algebrenklassen mit zueinander primen Diskriminanten*, Proceedings of the Imperial Academy of Japan, vol. 10 (1934), pp. 443–446.

† H. Hasse, *Über p-adische Schiefkörper und ihre Bedeutung für die Arithmetik hyperkomplexer Zahlsysteme*, Mathematische Annalen, vol. 104 (1931), pp. 495–534, Theorem 47.

THE UNIVERSITY OF CHICAGO,
CHICAGO, ILL.